İNTERNETİN BİLİNÇLİ KULLANIMI

PERSONEL SEMİNERİ

ÖZDEN KURTOĞLU
BİLİŞİM TEKNOLOJİLERİ ÖĞRETMENİ

E-GÜVENLİK NEDİR?

Karşıdan gelecek zararlara karşı farkında olup önlem alarak bilinçli bir şekilde internet kullanmayı sağlamaktır.

Bilişim cihazlarını kullanırken;

- Güvenlik duvarı kullanın.
- Önemli bilgileri yedekleyin.
- Antivirüs programı kullanın
- Emin olmadığınız e-posta eklerini açmayın.
- Güvenilir olmayan sitelerden indirme işlemi yapmayın.
- Güncel işletim sistemi kullanın.
- Flash bellek kullanırken her seferinde antivirüs taraması yapın.
- Aileniz için internet sağlayıcılardan aile veya çocuk paketlerini temin edin.

- Sistem yavaşlıyorsa;
- Bilgiler kayboluyorsa;
- İstenmeyen programlar, internet sayfaları açılıyorsa;
- Bilgisayar verdiğiniz komutları yerine getirmiyorsa;
- Bilgisayar isteğiniz dışında işlem yapıyorsa;
- Bazı dosyalar açılmıyorsa;

bilgisayarınıza zararlı yazılım bulaşmış olabilir!

Bilgisarımızı, zararlı yazılımlardan korumak ve zararı en aza indirmek için;

- GÜVENLİK DUVARI KULLANIN,
- ÖNEMLİ BİLGİLERİNİZİ YEDEKLEYİN,
- İŞLETİM SİSTEMLERİNİZİ GÜNCELLEYİN,
- ANTİVİRÜS PROGRAMI KULLANIN VE GÜNCEL TUTUN,
- EMİN OLMADIĞINIZ ELEKTRONİK POSTA EKLERİNİ AÇMAYIN,
- GÜVENİLİR OLMAYAN SİTELERDEN PROGRAM / MÜZİK / OYUN İNDİRMEYİN,
- TARAYICINIZIN GÜVENLİK AYARLARINI ÜST DÜZEYDE TUTUN,
- AYNI ANDA BİRDEN FAZLA ANTİVİRÜS PROGRAMI KURMAYIN,
- BULAŞMIŞ VİRÜSÜ TEMİZLEYEMİYORSANIZ BAŞKA ANTİVİRÜS PROGRAMLARI DENEYİN VEYA İŞLETİM SİSTEMİNİ BİÇİMLENDİRİN.

Zararlı Yazılımları Nasıl Fark Ederiz ve Korunuruz? / Bilişim Teknolojileri

eba

Virüs
Çalıştığında bilgisayarınıza değişik şekillerde zarar verebilen bilgisayar programlarıdır. Tüm virüsler, bir sistemde aktif hale geçirildikten sonra çoğalma özelliğine sahiptirler.

Truva Atı (Trojan)
Güvenli görünen ancak giriş yaptığı sistemin arka planına sızarak bilgisayarda olan biten tüm verileri internet korsanlarına sunabilen yazılımlardır.

Solucan (Worm)
Kendisini bir bilgisayardan diğerine kopyalamak için tasarlanmış ve bunu otomatik olarak yapan yazılımlardır. Solucanların en büyük tehlikesi, kendilerini büyük sayılarda çoğaltma becerileridir.

Casus Yazılımlar(SpyWare)
Tanıtım, kişisel bilgi toplama veya onayınızı almadan bilgisayarınızın yapılandırmasını değiştirme gibi belirli davranışları gerçekleştiren yazılımlardır. Casus yazılımlar, genellikle başka bir program kurulurken, sizin de onayınızla bilgisayarınıza kurulan yazılımlardır.

Reklam Yazılımları(AdWare)
Bilgisayarınızda reklamlar görüntülemek, arama isteklerinizi reklam web sitelerine yeniden yönlendirmek ve özelleştirilmiş reklamların görüntülenmesi için ziyaret ettiğiniz web sitelerinin türleri gibi hakkınızdaki pazarlama verilerini toplamak amacıyla tasarlanmış yazılımlardır.

GÜVENLİ ŞİFRE ÖZELLİKLERİ

Şifrenizi, tahmin edilebilir (doğum tarihi, doğum yeri, v.b.) bilgilerden oluşturmayın.

Herhangi bir yerde "şifrelerim", "passwords" gibi isimlerle oluşturulmuş belge bulundurmayın.

Şifrenizi hatırlatan güvenlik sorularını kolay tahmin edilecek bilgilerden oluşturmayın.

e-posta ve sosyal ağ şifrelerinizi mutlaka farklı oluşturun.

Şifrenizi en az 8 karakterden, içeriğini ise büyük harf,küçük harf, sayılar ve sembollerden oluşturun.

SOSYAL MEDYA KULLANIRKEN;

- İnternetten kimseyle tanışıp görüşmeyin.
- Rahatsızlık veren şahısları ihbar et.
- Tanımadığın kişilerden eposta, resim ve dosya kabul etme.
- İnternetteki kişilere hemen inanmayın.
- Özel bilgilerinizi asla paylaşmayın.
- Sosyal medyadan alışveriş yaparken sayfanın güvenilirliğine dikkat edin.
- Ailenizdeki ve okulunuzdaki reşit olmayan bireyleri sosyal medya konusunda uyarın.

SOSYAL AĞLARIN GÜVENLİ KULLANIMI

Link Kontrolü
Maddi değeri olan bir şey internette ücretsiz olamaz. Bu yönde ekrana gelen her linke tıklamayın, link kontrolü önlemini uygulayın.

Bilgi Paylaşımı
İlgili ayarları yapmadığınız takdirde ev / işyeri adres, telefon bilgilerinizin herkes tarafından görüleceğini unutmayınız.

Güvenlik Ayarları
Sosyal ağların yaptıkları güncellemeler ile güvenlik seviye ayarlarınızın değişebileceğini unutmayın.
Güvenlik ayarlarınızı kontrol edin.

Virüs Taraması
Sohbetlerde gönderilen her türlü belgeyi önce virüs taramasından geçirip sonra acın.

"Önce Düşün Sonra Paylaş"
Paylaştığınız her şeyin, kayıt olurken kabul ettiğiniz kurallar kapsamında haklarını devrettiğiniz site sunucusu üzerinde, kaldığını unutmayın.

Ücretsiz Uygulama
İnternetten indirilen ücretsiz uygulamalara her zaman güvenmeyin, bazı programların geri planda kimlik bilgilerini, şifreleri ve arkadaş listenizi alabileceğini unutmayın.

SİBER ZORBALIK

- Zorbalık içeren mesajları okumayın, beğenmeyin, başkalarıyla paylaşmayın
- Yazdıklarınızın karşı tarafı incitebileceğini, depresyona sokabileceğini düşünün.
- Kişilerin yüzüne söyleyemediklerinizi sanal ortamda da söylemeyin.
- Siber zorbalığın bir suç olduğunu, şikayet halinde ceza alabileceğinizi unutmayın.
- Gerçek hayatta nasıl davranıyorsanız, sanal ortamda da öyle davranın.
- Telif hakkına sahip olmadığınız içerikleri paylaşmayın.
- Başkalarının özel durumlarını paylaşmayın.

SİBER TUZAKLARI NASIL ANLARIM?

1. İnternette kimlik bilgilerini isteyen web sitelerine karşı dikkatli ol.

2. Bedava hediyelerden, programlardan ve kazanacağını söyleyen yarışmalardan uzak dur.

3. Eğlenceli gibi görünen testler, senin hakkında bilgi toplamak için hazırlanmış olabilir. Bir kez daha düşün.

4. Unutma! Bilinen markalar veya kurumlar e-posta yoluyla senden parola kimlik bilgileri gibi kişisel bilgiler istemez.

5. Açılır pencerelerle (pop-up) gelen yarışma ve anketlere katılma.

6. Şüpheli bulduğun e-postaların içindeki bağlantıya (linke) tıklama ve gönderilen dosyayı açma.

7. Tanımadığın kişilerden gelen e-postaları açmadan önce, tekrar düşün ve gönderilen dosyayı açma.

8. İçeriği arkadaşlarına da göndermeni isteyen e-postalar, seni ve arkadaşlarını riske atabilir. E-postayı sil ve arkadaşlarını uyar.

9. İsteğin dışında bilgisayar kameranın açılmaması için, kameranı kontrol et.

10. Oyun oynamak için, üye olmanı isteyen siteleri önce dikkatlice incele.

İNTERNETTE ÖNCE DÜŞÜN SONRA PAYLAŞ!!!

Güvenli İnternet Merkezi

D — Paylaştığımız bilgilerin doğruluğundan emin olmalıyız.

Ü — Faydalı ve gerekli bilgiler içeriyor mu kontrol etmeliyiz.

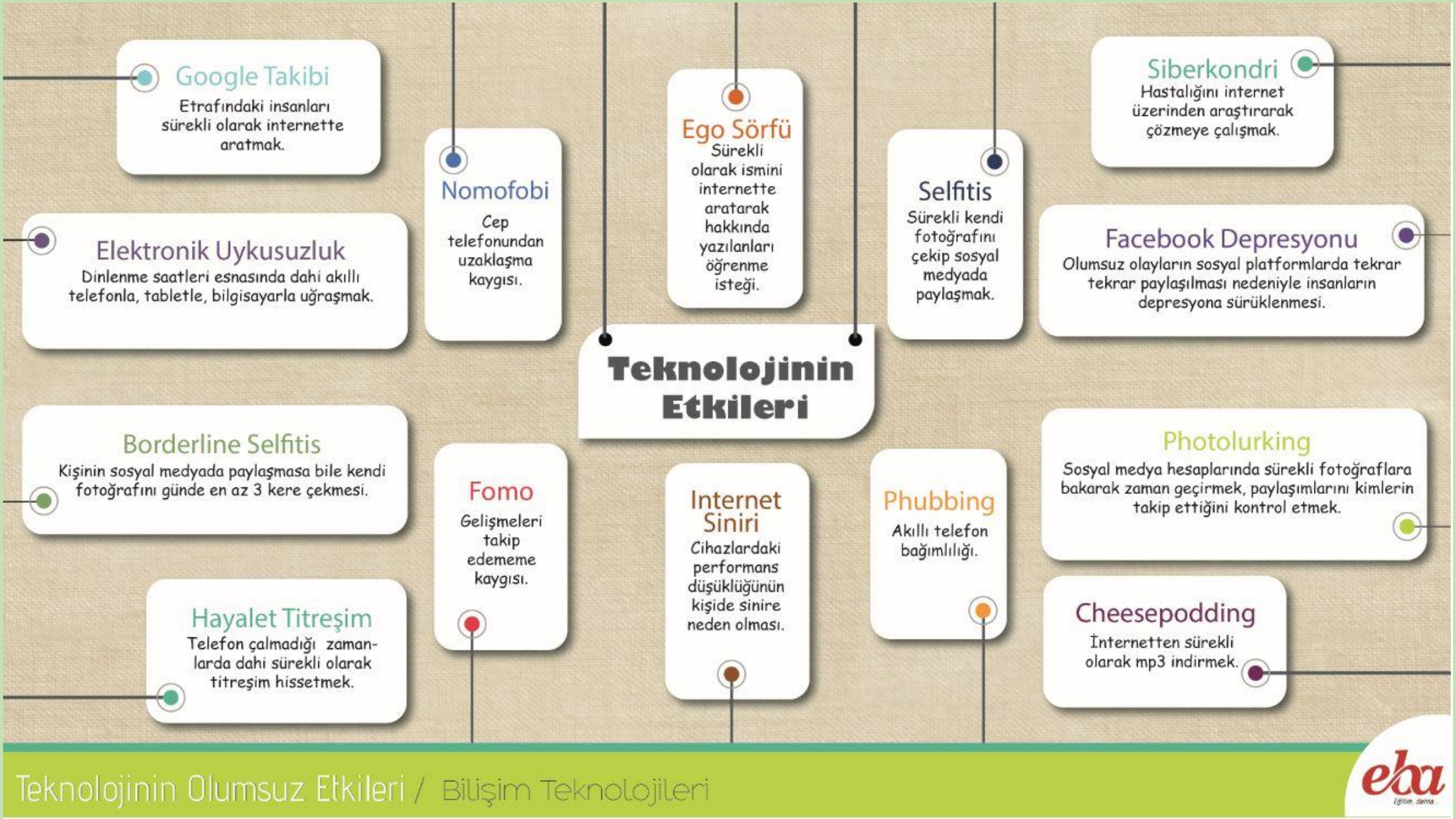
Ş — Kimlik bilgileri, telefon numarası gibi özel bilgiler içermemesine dikkat etmeliyiz.

Ü — Arkadaşlarımızı, ailemizi üzecek, incitecek paylaşımları yapmamalıyız.

N — Türkçe'yi düzgün kullanmaya, argo kelimeler ve kaba bir dil kullanmamaya özen göstermeliyiz.

www.guvenliweb.org.tr

www.gim.org.tr



Teknolojinin Olumsuz Etkileri / Bilişim Teknolojileri

YALAN HABER NASIL TESPİT EDİLİR?

DOĞRULAYIN!

Bir haberin doğruluğundan emin olmak için, aynı habere güvenilir başka kaynaklardan da ulaşabilmelisiniz. Haberi, güvenilir farklı kaynaklardan teyit edin.

KAYNAK GÜVENİLİR Mİ?

Haberin kaynağı ne, kaynağı kim?
İletişim bilgileri ve "Hakkında" bilgisi olmayan kaynaklara güvenmeyin.

ELEŞTİREL VE ŞÜPHECİ OLUN!

Şüpheci olun ve eleştirel bir bakış açısı edinin.
Öncelikle sorgulayın çünkü ulaşılan her bilgi doğru değildir.

HEMEN İNANMAYIN!

İnternette ve sosyal medyada gördüğünüze ve duyduğunuza hemen inanmayın.
Haber hakkında arka plan bilgileri edinin, gerekirse resmi ve birincil kaynaklarla iletişime geçin.

TARİHİ İNCELEYİN

Yalan haberlerdeki tarih ve saatler değiştirilmiş veya tutarsız olabilir.
Tarihe, yere ve görsellere dikkat edin.

EMİN OLMADAN PAYLAŞMAYIN!

Bazı haberler yönlendirme, yanıltma ve provokasyon amacı taşıyor olabilir.
Doğruluğundan ve ne amaçla dolaşımda olduğundan emin olmadan paylaşmayın!

İDDİALI BAŞLIKLARA DİKKAT!

Olağan dışı iddialar, ilgi çekmek için abartılmış başlıklar ve
çok fazla kullanılan noktalama işaretleri, genellikle asılsız haberlere aittir.

URL / ADRES GERÇEK Mİ?

Sahte haber siteleri genellikle güvenilir haber kaynaklarına çok benzeyen
taklit bir adres (URL) kullanırlar. İnternet adreslerine dikkat edin.

GÖRSELLERİ DOĞRULAYIN

Sahte haberler montajlanmış, garip görüntüler veya videolar içeriyor olabilir.
Görselleri doğrulamak için arama motorlarında aratarak fotoğrafın
ne zamana ait olduğunu, ne zaman yayınlandığını görebilirsiniz.

PARODİ VEYA REKLAM MI?

Bazı web siteleri parodi, reklam veya sahte haber yapıp yayma amacıyla kuruluyor.
Haberlere bunun bilincinde olarak yaklaşın.

GÜVENLİ İNTERNET MERKEZİ

GÜVENLİ İNTERNET BİLGİLENDİRME LİNKLERİ

- https://www.guvenlicocuk.org.tr/
- https://www.ihbarweb.org.tr/
- http://kesancumhuriyetortaokulu.meb.k12.tr/icerikler/bilincli-internet-kullanimi-e-brosurleri_10283160.html
- https://www.esafetylabel.eu/login

- KATILIMINIZ İÇİN TEŞEKKÜRLER.

ÖZDEN KURTOĞLU
BİLİŞİM TEKNOLOJİLERİ ÖĞRETMENİ